The Right Approach to Zero Trust Security for Enterprise IoT Devices

Table of Contents

Introduction

The incredible growth of the Internet of Things has presented unique business opportunities and new operational models across various industries and use cases. Although estimates vary, the Gartner Machina IoT database predicts there will be over 18 billion connected devices in enterprises by 2030. To put the numbers in perspective, by 2030, there will be four times the number of devices connecting to the network than the users in an enterprise.

These devices are powering exciting new use cases across a multitude of industries, from manufacturing to banking, as well as driving business outcomes and operational efficiencies previously unattainable. However, this explosion in adoption has inadvertently expanded the surface for cyberattacks, exposing organizations to a wide range of network-connected device security risks.

Palo Alto Networks Unit 42 IoT Threat Report, based on 1.2 million endpoints, found that IoT devices comprised 30% of all enterprise devices in 2020. On top of that, the Gartner Machina IoT database also predicts approximately 13% CAGR growth of IoT devices from 2020 to 2030.

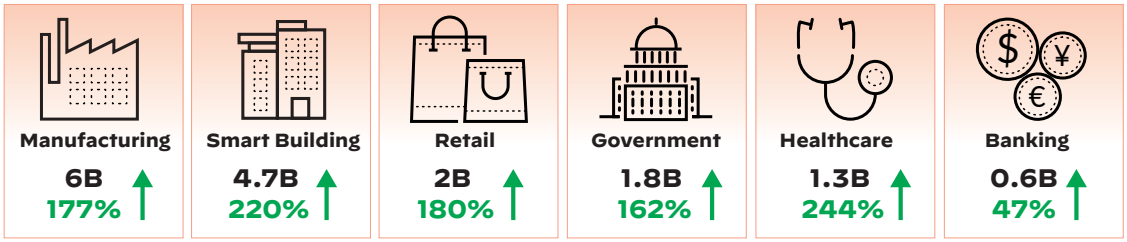

Figure 1: Projected IoT growth by industry, according to Gartner's Machina IoT Forecast database

Across all industries, the security risk exposure of these network-connected devices is high. Palo Alto Networks Unit 42's IoT Threat Report found that:

- 57% of IoT devices are highly vulnerable.
- 98% of all connected device traffic is unencrypted.
- 83% of connected devices run unsupported OS.

Security approaches historically employed by networking and security teams cannot effectively protect network-connected devices. These systems relied on protections at the network perimeter to secure organizations. The internal network was deemed trusted and secure, and application traffic could flow unrestricted. However, with the rise of connected devices and other changes, such as connectivity to the internet, cloud migration, and hybrid work, the traditional network perimeter is no longer a circle of trust.

To provide adequate security, the enterprise IT and security teams must account for all types of devices accessing the network, from conventional IT devices to connected IoT devices. The way to do this is by adopting a Zero Trust approach to security and applying it to network-connected devices and systems.

What Is Zero Trust Security

Zero Trust is a cybersecurity strategy that secures an organization by eliminating implicit trust and continuously validating every stage of digital interaction. The Zero Trust security approach is based on the principle that no user, device, or transaction from inside or outside the network can be assumed to be authorized. Eliminating implicit trust through a Zero Trust approach fosters a consistent security policy regardless of the situation. The Zero Trust framework focuses on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.

Traditional security models target the protection of the entire attack surface, which is difficult to identify and constantly evolving—especially when it includes network-connected devices. In a Zero Trust frame-

work, a "protect surface" is defined. It comprises the enterprise's most critical and valuable data, assets, applications, and services. Because it contains what is most critical to an organization's operations, the protect surface is orders of magnitude smaller than the attack surface and is always knowable.

Figure 2: Zero Trust principles for IoT devices

In Zero Trust, only known, allowed traffic can access the protect surface. In this case, IoT devices only have access to the data and applications they need to perform their tasks but nothing more. This is known as least-privileged access.

Zero Trust provides a security framework for network-connected devices that continuously validates their integrity. Zero Trust also enforces least-privileged access for connected devices, limiting exposure of data and applications. With Zero Trust, connected devices' transactions are secure and validated to thwart cyberthreats and protect data.

Palo Alto Networks has outlined the Zero Trust framework with the following guiding principles that encompass security for all users, applications, and infrastructure within an organization across the four pillars of Identity, Device/Workload, Access, and Transaction, as represented in table 1. These pillars are also applicable to IoT devices.

Securing unmanaged network-connected devices is essential to achieving Zero Trust for infrastructure. These guiding principles help define actionable Zero Trust security for all connected devices.

Table 1: Key Zero Trust Capabilities and Continuous Validation

	Identity	Device/Workload	Access	Transaction
Zero Trust for Users	Validate users with strong authentication	Verify user device integrity	Enforce least-privileged user access to data and applications	Scan all content for malicious activity and data theft
Zero Trust for Applications	Validate developers, DevOps, and admins with strong authentication	Verify workload integrity	Enforce least-privileged access for workloads accessing other workloads	Scan all content for malicious activity and data theft
Zero Trust for Infrastructure	Validate all users with access to the infrastructure	Identify all devices including IoT	Least-privileged access segmentation for native and third-party infrastructure	Scan all content within the infrastructure for malicious activity and data theft

The Right Approach to Zero Trust Security for Enterprise IoT Devices

The Zero Trust guiding principles outlined in the previous section translate into further granular guiding principles specific to achieving Zero Trust for office IoT and other devices such as printers, cameras, tablets, smart TV, HVAC systems, etc. Table 2 presents a Zero Trust framework that organizations should consider for securing network-connected devices.

Table 2: Zero Trust for Infrastructure Extended to Enterprise IoT Devices

Device/Workload	Access	Transaction
Discover all IoT devices	Recommend Zero Trust policies	Continuously monitor IoT devices
Assess IoT security risk	Enforce Zero Trust policies	Prevent known and unknown threats

Challenges in Implementing Zero Trust Security for IoT Devices

1. **Hard to Discover and Identify**
   - » Traditional agent-based endpoint security solutions cannot discover and manage IoT devices. Because of the low processing power and CPU for most IoT devices, they cannot have an endpoint agent installed on them.
   - » Most IoT security technologies only discover and classify the devices for which they have prepopulated signatures. Unfortunately, approaches based on device fingerprinting or signatures cannot scale to discover all connected devices because of the sheer variety of operating protocols, standards, and newer types of devices coming onto the network.
   - » Network-connected devices are rarely assigned a unique hardware identifier (unlike IT devices) and are manufactured in batches. Given this, most of these devices remain undiscovered or unidentified and unaccounted for in an IT team's device inventory.
2. **Hard to Authenticate, Define Policy, and Segment**
   - » Most network-connected devices do not support traditional enterprise authentication and authorization processes, such as 802.1X or single sign-on. Additionally, the MAC Authentication Repository (MAR) list does not work either due to poor device classification. Since connected devices are business enablers, network teams must onboard them manually without thoroughly risking their risk posture.
   - » Segmentation policies and rule creation require hours of manual work. Furthermore, the limited visibility into unmanaged devices makes it difficult to segment them properly.
3. **Hard to Continually Assess**
   - » Connected devices remain out of vulnerability scanner scope due to the vulnerability management solution's inability to detect them.
   - » Many network-connected devices are part of an organization's critical infrastructure, and active probing or scanning of these devices for risk and vulnerability assessment could also result in operational disruption.
4. **Lack of Zero Trust Capabilities**
   - » Existing network security solutions do not have the intelligence or capability to recommend Zero Trust risk reduction policies. It is up to the security teams to gather device insight and context and create Zero Trust policies manually. That can be a long and error-prone process.
   - » Many security solutions are alert-only and lack built-in prevention of threats and enforcement of Zero Trust security policies.

Addressing Challenges with Zero Trust for IoT Devices

Palo Alto Networks Enterprise IoT Security brings IoT devices into the Zero Trust security model fold and addresses challenges following principles based on three core areas:

1. Device/Workload
2. Access
3. Transaction

The principles behind these pillars minimize connected device security risks to keep your organization safe from cyberattacks. Palo Alto Networks has made it exceedingly easy to achieve Zero Trust for IoT devices, thus elevating organizations' overall security posture. The following is the Palo Alto Networks practical approach to how organizations can achieve Zero Trust for IoT devices.

Zero Trust Principle One: Identify All Connected Devices

Discovery

You can't secure what you can't see. To extend the principles of Zero Trust to IoT devices, it is essential to go beyond users and standard IT devices to include all unmanaged connected devices. Enterprise IoT Security from Palo Alto Networks is the only agentless IoT security solution that uses machine learning (ML) and deep packet inspection with crowdsourced telemetry to discover and classify every connected device in the network, including the never-seen-before ones.

ML is not only a superior approach compared to the reactive, traditional, signature-based device discovery methods, but it is also vital. The volume of network-connected devices unknown to IT is staggering, and the growth continues. An ML-powered device discovery approach ensures that new devices are quickly and accurately discovered and classified in real time. It provides an approach that addresses the challenges associated with new connected device types being added to the network, fueled by emerging wireless protocols, such as 5G.

Our Enterprise IoT Security analyzes 200 parameters to accurately match each connected device's IP address with its type, vendor, and model to surface 50+ essential device attributes that completely profile the device. Accurate and granular device classification is necessary to differentiate unmanaged network-connected devices from managed IT assets. Doing that enables enforcement of Zero Trust-driven security policies that only allow approved traffic across your network.

Figure 3 shows the top categories of contextual information that Enterprise IoT Security provides.

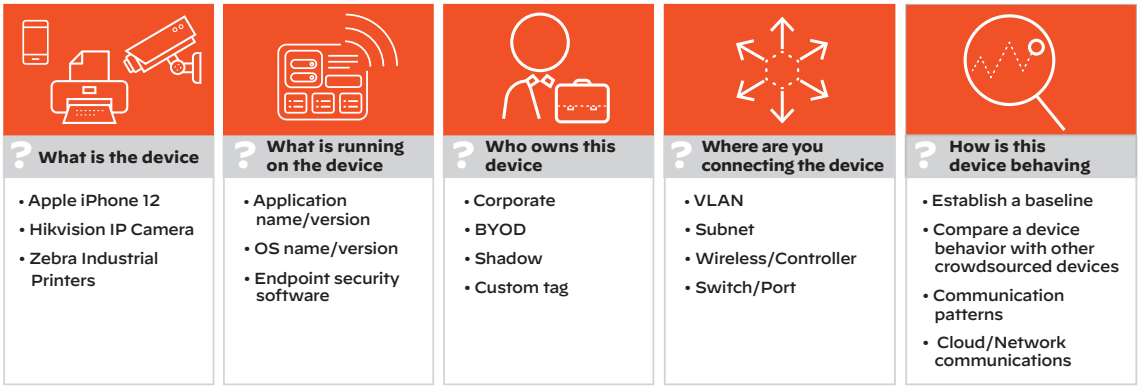

Figure 3: Enterprise IoT Security can discover 90% of the devices within 48 hours—and more after that

Risk Assessment

The next step in applying the Zero Trust framework is to assess the risk with high confidence and determine the level of risk for IoT devices. However, to assess risk effectively, one needs to know what it means, clarifying it relative to threats and vulnerabilities.

Risk is a function of threats exploiting vulnerabilities to compromise or damage assets, such as connected devices. Three vectors are used to measure network-connected device risk:

1. Threats
2. Vulnerabilities
3. Asset context

Enterprise IoT Security from Palo Alto Networks detects and assesses risk across all three vectors. This is done by leveraging crowdsourced device data, machine learning-powered device behavior anomaly assessment, proprietary Unit 42 threat research, CVEs, third-party vulnerability management information, and more.

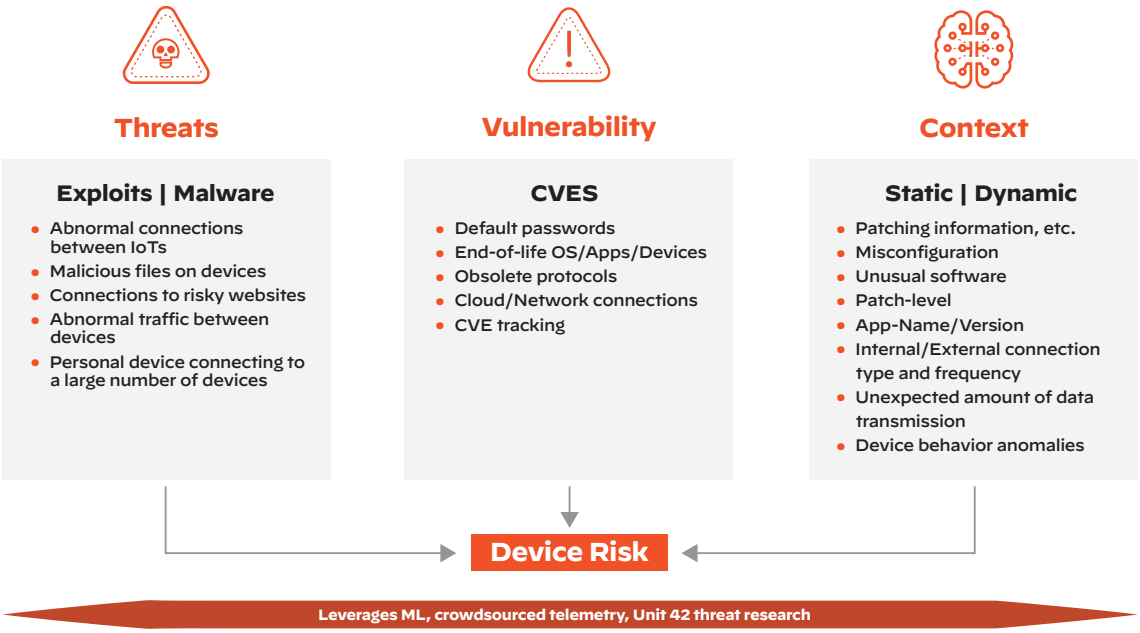

Figure 4: Enterprise IoT Security detects and assesses risk across these three vectors

Enterprise IoT Security measures risk and assigns a score for the amount of risk it observes at four levels:

1. Individual office IoT and other generic devices
2. Device profile
3. Site
4. Organization

When calculating the risk scores of IoT device profiles, sites, and organizations, Enterprise IoT Security considers the scores of individual devices within a particular group and the percentage of risky devices in the group. The different scores provide a simple means to check the risk posed at various points and areas of your network.

Discover IoT device vulnerabilities in your network in a few hours rather than three-plus weeks. Here's how.

Zero Trust Principle Two: Access

Least-privileged access segmentation for native and third-party infrastructure.

The Least Access Policy

The least access as a policy is a key tenet of Zero Trust. The least access as an Enterprise IoT Security policy is intended to offer a minimum level of network access by an IoT device. Since most IoT devices are "purpose-built" and have predictive behavior, least access policy can be used in the following scenarios:

- **Virtual patching (to keep IoT devices operational)**: The least access policy can allow even vulnerable connected IoT devices to operate by blocking or restricting their access to specific resources. This is a temporary strategy to limit the exploitation of a vulnerability while it is remediated.
- **Network access control policy**: The least access policy is also used to limit or restrict the access of network-connected IoT devices to specific resources to carry out their required task.

Today, one has to go through multiple labor-intensive steps to define and develop risk reduction policies per device profile. The manual steps include inventorying IoT devices, defining device profiles by device type or function, establishing behavioral baselines, defining policies that do not disrupt patient care or operations, and integrating with other technologies to enforce those policies. It also includes gathering the application usage, connection, and port/protocol data needed to create policies for each device.

Enterprise IoT Security from Palo Alto Networks is the only solution in the market today that goes beyond risk assessment to automatically provide least access policies. By comparing metadata across millions of connected devices with those found in your network, Enterprise IoT Security can use its device profiles to determine normal behavior patterns. Then, for each IoT device and category of devices, it provides a recommended policy to restrict or allow trusted behaviors and helps implement Zero Trust strategies automatically. Once reviewed, a policy can be quickly imported by your ML-Powered NGFW, and any changes will be updated automatically, keeping your administration overhead to a minimum.

Read how you can have 20X time savings from the automated policy creation of Enterprise IoT Security.

Network Segmentation Policy

Segmenting IoT devices can be viewed as a step toward the Zero Trust guiding principle of "never trust, always verify." For instance, running mission-critical sensors on the same network as printers would not be sound practice. A device profile-based segmentation approach that considers many factors, including device type, function, mission criticality, and threat level, provides an isolation approach that significantly reduces the potential impact of cross-infection by cyberthreats.

Enterprise IoT Security enabled on the Palo Alto Networks Next-Generation Firewall takes a device profile-based fine-grained segmentation approach that considers those factors to enable sequestration. This significantly reduces the potential impact of cross-infection between IT and IoT devices. In addition, using a Palo Alto Networks Next-Generation Firewall (NGFW) as a segmentation gateway leverages its inherent networking capabilities for seamless deployment into an existing environment and allows for the controlled introduction of security controls over connected devices within a network.

For customers who prefer to choose a network access control (NAC) solution to segment their network, Enterprise IoT Security provides built-in integration with Cisco ISE, Forescout, and Aruba ClearPass to implement segmentation. Enterprise IoT Security provides discovered unmanaged device information to the NAC solution and additional device context to segment them intelligently. This addresses the limitation of NAC only having visibility into devices that can be authenticated by eliminating blind spots for IoT devices that cannot be authenticated as they do not have users associated with them.

In addition, context-aware partitioning of IoT devices ensures they have least-privileged access and have access to only the required applications. It keeps them quarantined from guest and business networks and minimizes operational downtime for critical IoT devices by mitigating incompatibility issues that crop up between systems.

Policy Implementation

Enterprise IoT Security can natively implement recommended Zero Trust security policies with its NGFW or via third-party enforcement points in two primary ways:

1. Enforce recommendations with one click via Palo Alto Networks NGFW. Our patented Device-ID policy construct tracks an individual device across the network, providing detailed information as a context within the ML-Powered NGFW for any alert or incident that may occur—regardless of changes to the device's IP address or location. In addition, policy rules and Layer 7 controls are automatically updated as the location and identified risks change. Table 5 shows how Device-ID is more scalable and provides faster remediation and response to threats.
2. Enforce the recommended policies using our NAC integrations with Cisco ISE, Forescout, or Aruba ClearPass.

Table 3: How Device-ID Helps Administrators Get Fast and Accurate Policy Implementation

Without Device-ID	With Device-ID
Reliance on IP address as a proxy for device identity does not provide accurate device identity	Device identity is available within policy
Reliance on users, network, or device admins to properly address device issues is error-prone and creates an opportunity for exploitation	Consistent policy enforcement regardless of where the device is connected or how it is configured
Reliance on external systems such as NAC or asset management requires integrations to be built and maintained	Directly feed Device-ID using Enterprise IoT Security, eliminating the need for complex integrations
Threat or incident investigation needs SOC to touch multiple systems to track down which specific device generated the alert	Threats alert with device info received by SIEM

Zero Trust Principle Three: Transaction

Scan all content within the infrastructure for malicious activity and data theft.

Continuous Monitoring

Continuous monitoring is the final and crucial step in closing the Zero Trust security loop for network-connected IoT devices. Even if a device has been profiled and placed in the correct segment, it could still be compromised during its connection to the network. If an IoT device is compromised, its access to the resources and the network is immediately blocked.

Our ML-based Enterprise IoT Security automatically ascertains an IoT device's identity and verifies normal behaviors. Once normal behaviors are established, the solution kicks in anomaly detection to uncover and prioritize any potential deviation from the baseline. Our machine learning establishes a baseline of Layer 7 device behaviors and provides two types of insights:

1. Enterprise IoT Security uses ML to compare the behaviors with similar crowdsourced devices to establish a behavior baseline and monitor deviation continually. This information helps automate Zero Trust policy creation.
2. Enterprise IoT Security also monitors device traffic and communication patterns and continually contrasts them against existing VLAN designs to simulate the right microsegmentation design and, after that, enforcement.

IoT devices generate unique, identifiable patterns of network behavior. Using machine learning and AI, Enterprise IoT Security recognizes these behaviors and identifies every device on the network. It then creates a rich context-aware inventory that is dynamically maintained and always up to date.

After identifying a device and establishing a baseline of its normal network activities, Enterprise IoT Security monitors network activity to detect any unusual behavior indicative of an attack or breach. If suspicious activity is detected, Enterprise IoT Security notifies administrators through security alerts in the portal. Depending on each administrator's notification settings, alerts are sent through email and SMS notifications. Enterprise IoT Security also blocks devices not compliant with the established security and compliance policy from accessing the network.

Built-in Prevention

Enterprise IoT Security monitors all connected devices and stops all threats with the industry's leading IPS, malware analysis, web, and DNS prevention technology. Seamlessly integrated with Enterprise IoT Security, our Cloud-Delivered Security Services coordinate intelligence to prevent all network-connected device threats without increasing the workload for your security personnel. To decrease response times, connected devices with validated threats can be dynamically isolated upon detection of threats by our ML-Powered NGFWs. This gives your security team time to form remediation plans without the risk of further infection from those devices.

Zero Trust Security for All IoT Devices in Enterprise Ecosystems

In the past, securing users, applications, and devices identifiable inside the network perimeter was the obvious thing to do. However, the explosion of unmanaged IoT devices in enterprises with blurred, ever-expanding network security perimeters sets a new paradigm. As a result, enterprises must embrace a new yet simplified approach to network-connected device security modeled steadfastly on Zero Trust best practices.

The Palo Alto Networks Zero Trust approach is the most comprehensive strategy—a strategic framework guiding security for connected devices. By applying the principle of least-privileged access to connected devices, the Palo Alto Networks Zero Trust approach allows organizations to extract the maximum benefit from all devices with the least risk of exposure to cyberthreats.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com